**AMENDMENTS TO THE SPECIFICATION**

Please amend the specification as follows.

***- At page 1, before line 1, replace the title with the following amended title and section title:***

~~Circuit arrangement with non-volatile memory module and method for en-/decrypting data in the non-volatile memory module~~ **CIRCUIT ARRANGEMENT WITH NON-VOLATILE MEMORY MODULE AND METHOD FOR EN-/DECRYPTING DATA IN THE NON-VOLATILE MEMORY MODULE**

**BACKGROUND OF THE INVENTION**

***- At page 1, line 10, replace the paragraph with the following amended paragraph:***

- having at least one code ~~R[ead]O[nly]M[emory]~~ Read Only Memory (ROM) module for storing at lease one ~~R[ead]O[nly]M[emory]~~ ROM code; and

***- At page 1, lines 18 through 26, replace the paragraph with the following amended paragraphs:***

**DESCRIPTION OF RELATED ART**

Conventionally, key codes necessary for encrypting or decrypting the contents of a ~~N[on]V[olatile]~~Non-Volatile (NV) memory module are either hard-coded, defined by means of fuse cells especially instantiated therefore or saved themselves in a specially protected area of the non-volatile memory module.

Each of these known procedures has disadvantages, however: in the case of hard-coded keys, the key code cannot be changed for different controller versions with different ROM codes; in the case of the more flexible definition of the key code in fuse cells or in the case of protected ~~E[lectrical] E[rasable] P[rogrammable] R[ead] O[nly] M[emory]~~ Electrical Erasable Programmable Read Only Memory (EEPROM) areas, the key length is limited as a result of cell or surface area requirements.

**SUMMARY OF THE INVENTION**

***- At page2, lines 4 through 11, replace the paragraphs with the following amended paragraphs:***

This object is achieved with a circuit arrangement having the features indicated in ~~claim 1~~ Figure 1 and by an en-/decryption method based thereon having the features discussed herein below ~~indicated in claim 6~~. Advantageous embodiments and expedient further developments of the present invention are identified herein as well, ~~in the respective dependent claims.~~

According to the teaching of the present invention, therefore, a completely new approach is disclosed to the generation of at least one especially long key for the en-/decryption of at least one ~~N[on]V[olatile]~~ NV memory module from ~~R[ead]O[nly]M[emory]~~ ROM code data, for example for embedded security controllers.

***- At page 2, line 32 through page 3, line 2, replace the paragraph with the following amended paragraph:***

Through double use of the ROM code as a source for long key codes, the security of the encryption or decryption of the ~~N[on]V[olatile]~~ NV memory module is increased by greater key lengths, without such a greater key length resulting in a corresponding additional surface area requirement for storing this key code.

***- At page 3, lines 15 through 33, replace the paragraphs with the following amended paragraphs:***

**BRIEF DESCRIPTION OF THE DRAWINGS**

As already discussed above, there are various possible ways of advantageously embodying and developing the teaching of the present invention. ~~Reference is made, in this regard, to the claims subordinate to claims 1 and 6, and the~~ The invention will be further described with reference to examples of embodiments shown in the drawings to which, however, the invention is not restricted. In the Figures:

Fig. 1 is a schematic block diagram of an example of an embodiment of a circuit arrangement according to the present invention, by means of which the en-/decryption method may be performed according to the present invention.

## DETAILED DESCRIPTION OF THE EXEMPLARY EMBODIMENTS OF THE INVENTION

Fig. 1 shows an example of an embodiment of a circuit arrangement 100 for electronic data processing; in particular, the circuit arrangement 100 is provided for use in a microcontroller of the "embedded security controller" type.

This circuit arrangement 100 comprises a multi-component ~~N[on]V[olatile]~~ NV memory module 10, which takes the form of an ~~E[lectrical] E[rasable] P[rogrammable] R[ead] O[nly] M[emory]~~ EEPROM and by means of which data may be stored which are to be protected from unauthorized access by encryption or decryption.

Assigned to this ~~N[on]V[olatile]~~ NV memory module 10 is a memory module interface logic circuit 12, by means of which

***- At page 4 lines 10 through 13, replace the paragraph with the following amended paragraph:***

In addition, the circuit arrangement 100 comprises a code ~~R[ead] O[nly] M[emory]~~ ROM module 20 for storing and supplying ~~R[ead] O[nly] M[emory]~~ ROM codes. Assigned to this code ROM module 20 is code ROM module interface logic circuit 22 by means of which

***- At page 4, lines 23 through 30, replace the paragraph with the following amended paragraph:***

To this end, the memory module interface logic circuit 12 comprises an en-/decryption logic circuit 14 having a key address generation unit 16 and a key register 18. The key address generation unit 16 is provided in this context for the purpose of generating an ROM key address (→ reference numeral 162a: ROM key address data from the key

address generation unit 16 to a multiplexing unit 24 of the code ROM module interface logic circuit 22) in the case of write or read access to the memory module 10 using a memory module address coming from the ~~C[entral]P[rocessing]U[nit]~~ Central Processing Unit (CPU) (→ reference numeral C12a: address data "CPU NV addr" from the CPU to the memory module interface logic circuit 12).

***- At page 6, lines 10 through 18, replace the paragraphs with the following amended paragraphs:***

For encryption (in the event of write access, reference numeral 120w) or decryption (in the event of read access, reference numeral 120r) of the NV memory data "DIN(d:0)" or "DOUT(d:0)", this ROM code byte is then used as a key byte or as part of the key byte, such that in an extreme case a key space is produced which is of exactly the same size as the code space of the ~~N[on]V[olatile]~~ NV memory module 10.

(ii) Generation of the key code in the reset phase, i.e. by ~~one off~~ one of reading out of particular ROM code bytes, in particular at the time of the reset sequence, and by storing these ROM code bytes in the key register 18 until the time of a write/read access to the memory module 10, i.e. until these ROM code bytes are required for a write operation or a read operation of the memory module 10:

***- At page 7, line 2, replace the paragraph with the following amended paragraph:***

10 ~~N[on]V[olatile]~~ NV memory module

***- At page 7, line 8, replace the paragraph with the following amended paragraph:***

20 Code ~~R[ead] O[nly] M[emory]~~ ROM module

***- Please replace the Abstract with the following amended Abstract:***

~~In order to further develop a circuit arrangement (100) for electronic data processing having at least one non-volatile memory module (10) for storing data to be protected against~~

~~unauthorized access by means of encryption or decryption having at least one code R[ead]O[nly]M[emory] module (20) for storing and/or supplying at least one R[ead]O[nly]M[emory] code; and having at least one code ROM module interface logic circuit (22) assigned to the code ROM module (20) and an en-/decryption method based thereon in such a way that on the one hand the key code may be changed for different controller versions with different ROM codes and on the other hand the length of the key code is not limited, it is proposed that the data assigned to the memory module (10) be encrypted or decrypted by means of the ROM code supplied by the code ROM module (20).~~ An apparatus and method is provided for protecting data in a non-volatile memory by using an encryption and decryption that encrypts and decrypts the address and the data stored in the non-volatile memory using a code read only memory that stores encryption and decryption keys that are addressed by a related central processing unit at the same time data is being written or read from the non-volatile memory by the central processing unit.